

HNS Newsletter
Issue 383 - 03.09.2007
<http://www.net-security.org>

This issue is sponsored by:

FREEMAP - Graphically Map & Understand Your Network

Do you know all the devices on your network perimeter?
Are there rogue devices exposing your critical assets?
Qualys' FreeMap provides a detailed network topology
of all your network devices that can be "seen" from the
Internet in graphic or text mode so you can take control
of your network perimeter and accurately inventory your
network assets.

Run a FreeMap today at:

<http://freemap.qualys.com/?lsid=7023>

Table of contents:

- 1) Security news
- 2) Advisories
- 3) Articles
- 4) Software
- 5) Webcasts
- 6) Conferences
- 7) Security World
- 8) Virus News

[Security news]

SPAM FIGHTERS HIT CRIMINALS' WEAK SPOT

Anti-spam groups want to target sources instead of relying on filters
to decrease stream of junk e-mail.

<http://www.net-security.org/news.php?id=15094>

HOW-TO: ENCRYPT AND HIDE A DISK PARTITION

Separate hard disk partitions can be used for any number of reasons.

<http://www.net-security.org/news.php?id=15095>

WINDOWS GENUINE ADVANTAGE SUFFERS WORLDWIDE OUTAGE

Microsoft is aware of a major WGA server outage affecting users across the globe.

<http://www.net-security.org/news.php?id=15096>

CHINA 'GRAVELY CONCERNED' BY GERMANY HACKING REPORTS

China's Premier Wen Jiabao on Monday expressed "grave concern" over reports that Chinese army hackers had penetrated German government computers systems and he vowed to crack down on such activity.

<http://www.net-security.org/news.php?id=15097>

SECURITY CRASHES INTO PRODUCTIVITY

Our manager didn't tell users that they could have laptops, but she's the one who has to tell them that they can't.

<http://www.net-security.org/news.php?id=15098>

DESIGNING A PCI-COMPLIANT LOG MONITORING SYSTEM

Log monitoring activities are an integral part of Requirement 10 of the PCI Data Security Standard and it can be difficult to understand how the different logging portions of Requirement 10 interrelate. Despite this fact, some organizations are seeking to redesign their PCI logging environment in order to best accommodate the PCI requirements. In this article we will examine a few key design points for architecting a log monitoring and management system that would be compliant with PCI Requirement 10.

<http://www.net-security.org/news.php?id=15099>

YOU DON'T WANT TO HEAR IT: 10 PIECES OF LOUSY SECURITY ADVICE

The customer strikes back: 10 things your security "experts" shouldn't be saying.

<http://www.net-security.org/news.php?id=15100>

TWO OPEN SOURCE EMAIL VIRUS SCANNERS FOR LINUX

If Linux is hardly affected by viruses, why do system administrators use anti-virus software on their Linux email servers?

<http://www.net-security.org/news.php?id=15101>

FACING UP TO SECURITY IN 3D

Researchers want to partner with businesses, particularly in the finance sector, to develop commercial real-time, high-speed facial recognition technology for security applications.

<http://www.net-security.org/news.php?id=15102>

SECURING SSH USING DENYHOSTS

SSH is a great way to remotely administer a server. However, it still has a number of issues when you open it up to the world.

<http://www.net-security.org/news.php?id=15103>

VIDEO GAMES THAT AID NATIONAL SECURITY

Scientists working on national security are developing a new generation of video games, ones they believe will train emergency personnel faster than existing methods.

<http://www.net-security.org/news.php?id=15104>

APPLE IPHONE ISSUE HIGHLIGHTS SECURITY DEBATE

What counts as private has to change if we're to get the most out of the network, argues Bill Thompson.

<http://www.net-security.org/news.php?id=15105>

I AM MY OWN PASSWORD

How identity issues get tied up in strings of letters and numbers.

<http://www.net-security.org/news.php?id=15106>

5 SECURITY WIDGETS FOR THE OPERA BROWSER

Widgets are Web programs you can run right on your desktop using Opera 9. This article introduces security-related widgets that will enhance your Opera experience.

<http://www.net-security.org/news.php?id=15107>

JAPAN MILITARY HOMES, DESTROYER RAIDED OVER DATA LEAK

The homes of several serving members of Japan's Maritime Self Defense Force (JMSDF) and a destroyer were raided as part of an investigation into a leak of sensitive military data from a computer.

<http://www.net-security.org/news.php?id=15108>

POINTS OF ATTACK: PHP AND AJAX

It's easy to get caught up in the dynamic potential of Ajax. But with innumerable possibilities also comes increased risk. If security isn't a major concern, it should be.

<http://www.net-security.org/news.php?id=15109>

WHY APPLE CAN'T STOP IPHONE HACKERS

Will Apple and AT&T's legal action deter hackers? Hardly.

<http://www.net-security.org/news.php?id=15110>

JUDGE: TORRENTSPY MUST PRESERVE DATA IN RAM

A federal judge has upheld a magistrate's decision forcing TorrentSpy to enable server logging so the Motion Picture Association of America can obtain the IP addresses of those connecting to BitTorrent files via the service.

<http://www.net-security.org/news.php?id=15111>

INTRODUCTION TO NETWORK-BASED INTRUSION DETECTION SYSTEMS

Bill Stallings covers the subject of network-based intrusion detection systems.

<http://www.net-security.org/news.php?id=15112>

WHY IT SECURITY MUST COMBAT ORGANIZED CYBERCRIME

Ditch the Hollywood stereotypes. These guys don't wear wide ties or spats, have flattened noses, or speak with strange accents. Nor do they have a fictional HBO series.

<http://www.net-security.org/news.php?id=15113>

ICANN'S WHOIS PRIVACY REFORMS STALLED AGAIN

Efforts to forge a compromise ended last week.

<http://www.net-security.org/news.php?id=15114>

INSIDE DCSNET, THE FBI'S NATIONWIDE EAVESDROPPING NETWORK

The FBI has quietly built a sophisticated, point-and-click surveillance system that performs instant wiretaps on almost any communications device, according to nearly a thousand pages of restricted documents newly released under the Freedom of Information Act.

<http://www.net-security.org/news.php?id=15115>

VIRTUAL PATCHING DURING INCIDENT RESPONSE: UNITED NATIONS DEFACEMENT

Virtual Patching is a policy for a web application firewall (in this case ModSecurity) that is able to identify attempts to exploit a specific Website vulnerability.

<http://www.net-security.org/news.php?id=15116>

SECURITY ECONOMICS

Information security has finally become mainstream. It is almost a recognized profession, with its own areas of specialization: network security, audit, incident response, forensics, and security management. Salaries for IS practitioners have been rising

constantly, the market for security products and services is large. The "security frontier" has moved from firewalls and anti-virus to IM and VoIP security. However, convincing people and organizations to implement effective security measures has not become easier, so we must ask ourselves — is security worth it?
<http://www.net-security.org/news.php?id=15117>

LAYERS IN IT SECURITY

A layered security strategy is a good practice to enhance the overall IT security in companies.
<http://www.net-security.org/news.php?id=15118>

ID FRAUD COSTING 'BILLIONS'

Identity fraud is costing Australia billions of dollars a year and nearly everyone is concerned about the theft and illegal use of their identity, federal Attorney-General Philip Ruddock says.
<http://www.net-security.org/news.php?id=15119>

FINDING SENSITIVE DATA AS A CONSULTANT WITH NESSUS

There are many consultants that use Nessus to scan a customer network for vulnerabilities and report a laundry list of security issues which need to be fixed.
<http://www.net-security.org/news.php?id=15120>

SATELLITE PHOTO SPARKS IMAGERY DEBATE

Throughout the Cold War, satellite and spy plane imagery of military sites was the sort of valuable, close-hold information that could start or stop a war or spawn a new arms race. Only those with top clearances saw them.
<http://www.net-security.org/news.php?id=15121>

LINUX CORPORATION SCAM TARGETS THE UNWARY

Be on guard against alleged representatives of Linux Corporation offering to buy your photos -- it's a scam.
<http://www.net-security.org/news.php?id=15122>

ANALYZING A SUSPECT WMF FILE

Randy Armknecht detected a malformed WMF file...
<http://www.net-security.org/news.php?id=15123>

MICROSOFT: VISTA SP1 COMING IN EARLY 2008

Putting to rest months of rampant rumors and speculation, Microsoft on Wednesday said it plans to launch the first service pack for

Windows Vista during the first quarter of 2008.
<http://www.net-security.org/news.php?id=15124>

LEGAL OR NOT, IPHONE HACKS MIGHT SPUR REVOLUTION
The iPhone's fantastic user interface is inspiring another consumer-electronics revolution: making people care about cell-phone unlocking.
<http://www.net-security.org/news.php?id=15125>

GERMAN LEFT SLAM EMAIL SPY PLAN
Left-wing members of the ruling coalition have objected strongly to plans by the German interior ministry to enlist email spy software to monitor terror suspects.
<http://www.net-security.org/news.php?id=15126>

REASONS FOR MAKING BACKUPS
Every company makes backups. However, I have seen several occasions where backups were not working as expected.
<http://www.net-security.org/news.php?id=15127>

AT&T LAPTOP THEFT EXPOSES EMPLOYEE DATA
AT&T and Maryland's Department of the Environment have become the latest organizations to find out first hand why security analysts for some time now have advocated the use of encryption to protect sensitive data on laptops and other mobile devices.
<http://www.net-security.org/news.php?id=15128>

INTRODUCING WINDOWS VISTA SERVICE PACK 1
The goal of Windows Vista SP1 is to address key feedback Microsoft has received from its customers without regressing application compatibility.
<http://www.net-security.org/news.php?id=15129>

REDUCING SHOULDER-SURFING BY USING GAZE-BASED PASSWORD ENTRY
Shoulder-surfing – using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information – is a problem that has been difficult to overcome. EyePassword is a system that mitigates the issues of shoulder surfing via a novel approach to user input.
<http://www.net-security.org/news.php?id=15130>

HANDS ON: SECURING APPLE'S OPEN DIRECTORY

Apple's Open Directory is a powerful directory services platform that supports a variety of clients, most notably Mac OS X and Windows.
<http://www.net-security.org/news.php?id=15131>

SPEED UP YOUR AJAX APPLICATIONS WHILE DODGING WEB SERVICES VULNERABILITIES

Judith Myerson gives a brief Ajax recap, shows what Web services vulnerabilities are and why Service Level Agreements (SLA) are important, and suggests some solutions for speeding up Ajax applications.

<http://www.net-security.org/news.php?id=15132>

[Advisories]

All advisories are located at:

http://www.net-security.org/archive_advi.php

Debian Security Advisory - pptpd (DSA 1288-2)

<http://www.net-security.org/advisory.php?id=7884>

Debian Security Advisory - clamav (DSA 1366-1)

<http://www.net-security.org/advisory.php?id=7883>

Debian Security Advisory - id3lib3.8.3 (DSA 1365-1)

<http://www.net-security.org/advisory.php?id=7882>

Debian Security Advisory - vim (DSA 1364-1)

<http://www.net-security.org/advisory.php?id=7881>

Mandriva Linux Security Update Advisory - clamav (MDKSA-2007:172)

<http://www.net-security.org/advisory.php?id=7880>

Debian Security Advisory - linux-2.6 (DSA 1363-1)

<http://www.net-security.org/advisory.php?id=7879>

Slackware Security Advisory - java (jre, jdk) ((SSA:2007-243-01)
<http://www.net-security.org/advisory.php?id=7878>

Ubuntu Security Notice - linux-source-2.6.20 vulnerabilities
(USN-510-1)
<http://www.net-security.org/advisory.php?id=7877>

SUSE Security Announcement - SUSE Security Summary Report
(SUSE-SR:2007:018)
<http://www.net-security.org/advisory.php?id=7876>

Ubuntu Security Notice - linux-source-2.6.15 vulnerabilities
(USN-508-1)
<http://www.net-security.org/advisory.php?id=7875>

Ubuntu Security Notice - linux-source-2.6.17 vulnerabilities
(USN-509-1)
<http://www.net-security.org/advisory.php?id=7874>

SUSE Security Announcement - opera (SUSE-SA:2007:050)
<http://www.net-security.org/advisory.php?id=7873>

Ubuntu Security Notice - tcp-wrappers vulnerability (USN-507-1)
<http://www.net-security.org/advisory.php?id=7872>

Debian Security Advisory - lighttpd (DSA-1362)
<http://www.net-security.org/advisory.php?id=7871>

Debian Security Advisory - postfix-policyd (DSA-1361)
<http://www.net-security.org/advisory.php?id=7870>

Apple Security Update - Firmware version 7.2.1 for AirPort Extreme
802.11n* base stations (APPLE-SA-2007-08-29)
<http://www.net-security.org/advisory.php?id=7869>

Cisco Security Response - VTY Authentication Bypass Vulnerability
<http://www.net-security.org/advisory.php?id=7868>

Cisco Security Advisory - XSS and SQL Injection in Cisco CallManager/Unified Communications Manager Logon Page (cisco-sa-20070829-ccm)
<http://www.net-security.org/advisory.php?id=7867>

Ubuntu Security Notice - enigma regression (USN-469-2)
<http://www.net-security.org/advisory.php?id=7866>

Ubuntu Security Notice - emacs21 vulnerability (USN-504-1)
<http://www.net-security.org/advisory.php?id=7865>

Ubuntu Security Notice - vim vulnerability (USN-505-1)
<http://www.net-security.org/advisory.php?id=7864>

Ubuntu Security Notice - tar vulnerability (USN-506-1)
<http://www.net-security.org/advisory.php?id=7863>

Mandriva Linux Security Update Advisory - kernel (MDKSA-2007:171)
<http://www.net-security.org/advisory.php?id=7862>

Debian Security Advisory - rsync (DSA-1360)
<http://www.net-security.org/advisory.php?id=7861>

Debian Security Advisory - dovecot (DSA 1359-1)
<http://www.net-security.org/advisory.php?id=7860>

=====

FREEMAP - Graphically Map & Understand Your Network

=====

Do you know all the devices on your network perimeter?
Are there rogue devices exposing your critical assets?
Qualys' FreeMap provides a detailed network topology of all your network devices that can be "seen" from the Internet in graphic or text mode so you can take control of your network perimeter and accurately inventory your network assets.

Run a FreeMap today at:

<http://freemap.qualys.com/?lsid=7023>

[Articles]

All articles are located at:

http://www.net-security.org/articles_main.php

Articles can be contributed to articles@net-security.org

REDUCING SHOULDER-SURFING BY USING GAZE-BASED PASSWORD ENTRY

Shoulder-surfing – using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information – is a problem that has been difficult to overcome. EyePassword is a system that mitigates the issues of shoulder surfing via a novel approach to user input.

<http://www.net-security.org/article.php?id=1063>

SECURITY ECONOMICS

Information security has finally become mainstream. It is almost a recognized profession, with its own areas of specialization: network security, audit, incident response, forensics, and security management. Salaries for IS practitioners have been rising constantly, the market for security products and services is large. The "security frontier" has moved from firewalls and anti-virus to IM and VoIP security. However, convincing people and organizations to implement effective security measures has not become easier, so we must ask ourselves — is security worth it?

<http://www.net-security.org/article.php?id=1062>

5 SECURITY WIDGETS FOR THE OPERA BROWSER

Widgets are Web programs you can run right on your desktop using Opera 9. This article introduces security-related widgets that will enhance your Opera experience.

<http://www.net-security.org/article.php?id=1061>

DESIGNING A PCI-COMPLIANT LOG MONITORING SYSTEM

Log monitoring activities are an integral part of Requirement 10 of the PCI Data Security Standard and it can be difficult to understand how the different logging portions of Requirement 10 interrelate.

Despite this fact, some organizations are seeking to redesign their PCI logging environment in order to best accommodate the PCI requirements. In this article we will examine a few key design points for architecting a log monitoring and management system that would be compliant with PCI Requirement 10.
<http://www.net-security.org/article.php?id=1060>

[Software]

Windows software is located at:
http://net-security.org/software_main.php?cat=1

Linux software is located at:
http://net-security.org/software_main.php?cat=2

Pocket PC software is located at:
http://net-security.org/software_main.php?cat=3

Mac OS X software is located at:
http://net-security.org/software_main.php?cat=5

AD-AWARE 2007 FREE (Windows)
Ad-aware is a free multi spyware removal utility.
<http://www.net-security.org/software.php?id=135>

JSCH 0.1.34 (Windows)
JSch is a pure Java implementation of SSH2.
<http://www.net-security.org/software.php?id=417>

MAILSCANNER 4.63.7-2 (Linux)
MailScanner is a virus scanner for e-mail designed for use on e-mail gateways.
<http://www.net-security.org/software.php?id=144>

MARADNS 1.2.12.08 (Linux)
MaraDNS is a DNS server that strives to be secure and fully open-sourced.
<http://www.net-security.org/software.php?id=84>

NAGIOS 3.0b3 (Linux)

Nagios is a host and service monitor designed to inform you of network problems before your clients, end-users or managers do.
<http://www.net-security.org/software.php?id=279>

PASSWORD SAFE 3.10 (Windows)

Password Safe is a password database utility.
<http://www.net-security.org/software.php?id=172>

SSL-EXPLORER 0.2.15.01 (Windows)

The 3SP SSL-Explorer is the world's first open-source SSL-based VPN solution of its kind.
<http://www.net-security.org/software.php?id=579>

STRONGSWAN 4.1.6 (Linux)

strongSwan is a complete IPsec and IKEv1 implementation for Linux 2.4 and 2.6 kernels
<http://www.net-security.org/software.php?id=643>

TOR, PRIVOXY AND VIDALIA BUNDLE 0.1.2.17 (Windows)

An anonymous Internet communication system.
<http://www.net-security.org/software.php?id=253>

TROUSERS 0.3 (Linux)

TrouSerS is a Trusted Computing Group Software Stack (TCG TSS) implementation.
<http://www.net-security.org/software.php?id=266>

WINSCP 4.0.4 (Windows)

WinSCP is an open source SSH file transfer protocol and secure copy client for Windows using SSH.
<http://www.net-security.org/software.php?id=6>

[Webcasts]

All webcasts are located at:

<http://net-security.org/webcasts.php>

Deploying Forefront Client Security (Part 1 of 2)
Organized by Microsoft on 5 September 2007, 11:30 AM
<http://www.net-security.org/webcast.php?id=492>

Deploying Forefront Client Security (Part 2 of 2)
Organized by Microsoft on 19 September 2007, 11:30 AM
<http://www.net-security.org/webcast.php?id=493>

[Conferences]

All conferences are located at:
<http://net-security.org/conferences.php>

HITBSecConf2007
Organized by Hack in the Box - 3 September-6 September 2007
<http://www.net-security.org/conference.php?id=226>

IMF 2007 - 3rd International Conference on IT-Incident Management &
IT-Forensics
Organized by SIDAR - 11 September-13 September 2007
<http://www.net-security.org/conference.php?id=233>

InfowarCon 2007
Organized by Interpact - 19 September-21 September 2007
<http://www.net-security.org/conference.php?id=225>

Information Security Solutions Europe / SECURE 2007
Organized by Revolution Events - 25 September-27 September 2007
<http://www.net-security.org/conference.php?id=227>

Smart Card Alliance Annual Conference 2007

Organized by Smart Card Alliance - 9 October-11 October 2007
<http://www.net-security.org/conference.php?id=231>

Secure Denmark 2007
Organized by ISSA - 9 October-9 October 2007
<http://www.net-security.org/conference.php?id=230>

Biometrics 2007 Conference & Exhibition
Organized by Elsevier - 17 October-19 October 2007
<http://www.net-security.org/conference.php?id=228>

Hack.Lu 2007
Organized by hack.lu - 18 October-20 October 2007
<http://www.net-security.org/conference.php?id=229>

RSA Conference Europe 2007
Organized by RSA Conference - 22 October-24 October 2007
<http://www.net-security.org/conference.php?id=222>

3rd Annual Techno Forensics Conference
Organized by The TrainingCo. - 29 October-31 October 2007
<http://www.net-security.org/conference.php?id=212>

Breakpoint Security Conference 2007
Organized by Breakpoint Security - 15 November-18 November 2007
<http://www.net-security.org/conference.php?id=232>

[Security World]

All security world articles are located at:
http://www.net-security.org/secworld_main.php

Send your press releases to press@net-security.org

Searching for evil

<http://www.net-security.org/secworld.php?id=5450>

Security update for AirPort Extreme 802.11n base station
<http://www.net-security.org/secworld.php?id=5449>

NSA Secure Workstation Solution to use VMware
<http://www.net-security.org/secworld.php?id=5448>

Best practices to combat SME security threats
<http://www.net-security.org/secworld.php?id=5447>

Is PDF spam simply not working for the spammers?
<http://www.net-security.org/secworld.php?id=5446>

Symantec releases Norton Internet Security 2008, Norton AntiVirus 2008
<http://www.net-security.org/secworld.php?id=5445>

Intel vPro processor technology fortifies security
<http://www.net-security.org/secworld.php?id=5444>

A closer look at Cryptainer LE: your own secure hidden data vaults
<http://www.net-security.org/secworld.php?id=5443>

Video: User Account Control in Windows Vista
<http://www.net-security.org/secworld.php?id=5442>

The state of data security in North America
<http://www.net-security.org/secworld.php?id=5441>

New web security and web filtering solutions for small businesses
<http://www.net-security.org/secworld.php?id=5440>

[Virus News]

All virus news are located at:
<http://www.net-security.org/viruses.php>

Malicious toolbars top the list of most common malware
http://www.net-security.org/virus_news.php?id=858

Company wins important ruling for the anti-malware industry
http://www.net-security.org/virus_news.php?id=857

Weekly malware report: MSN Messenger and IRC worms
http://www.net-security.org/virus_news.php?id=856

Rihanna and Kelly Clarkson video emails spread a trojan horse
http://www.net-security.org/virus_news.php?id=855

Up to 59% of companies with active malware on their networks
http://www.net-security.org/virus_news.php?id=854

Price list: trojans, password stealers, spam servers
http://www.net-security.org/virus_news.php?id=853

=====

FREEMAP - Graphically Map & Understand Your Network

=====

Do you know all the devices on your network perimeter?
Are there rogue devices exposing your critical assets?
Qualys' FreeMap provides a detailed network topology
of all your network devices that can be "seen" from the
Internet in graphic or text mode so you can take control
of your network perimeter and accurately inventory your
network assets.

Run a FreeMap today at:

<http://freemap.qualys.com/?lsid=7023>

=====

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

Unsubscribe from this weekly digest on:
<http://www.net-security.org/subscribe.php>

The archive of the newsletter in TXT and PDF format is available
http://www.net-security.org/newsletter_archive.php